swisscom

beem

Simply secure.

Enable, drive and protect
your business.

29.07.2026

Working securely from anywhere and protecting your business is finally simple.

beem, together with the integrated beemNet, is a comprehensive solution that securely networks and protects company sites, users, devices and data.
beem is a modular, innovative connectivity and security solution that combines the best mobile and fixed network connectivity, additional services and comprehensive security – all with the simplest set-up and no need for hardware or installation.

Protect all access to business applications and the Internet with an integrated, modular solution that works from anywhere. beem makes it easy for you to implement security guidelines company wide and to use comprehensive, seamlessly integrated security functions. Both end users and IT managers benefit from the ease of use and simple integration.

Comprehensive protection in beemNet

beemNet is your secure corporate network from Swisscom, provided and operated in Switzerland. The protection offered in beemNet goes far beyond the level of security currently found in most companies: all company sites, networks and devices connected to beemNet are automatically protected against cyberthreats and users can surf securely and stay anonymously. beemNet also enables you to benefit from comprehensive beem security functions.

Customised solutions for all companies

beem offers highly effective cybersecurity, seamlessly integrated into a modular solution for networking, communication and other services. Simply select the elements your company requires to enable your users to communicate easily and access data securely. State-of-the-art, effective, company-wide security is always included

Innovation and up-to-date security

The specialist knowledge of over 300 Swisscom security professionals ensures that beem is updated daily and continuously developed through the use of innovation. You no longer need to adjust security settings; with beem, you can simply rely on up-to-date protection against cyberthreats – now and always.

Enjoy transparent security

beem brings transparency to digital user data, averted cyberattacks and relevant security incidents. This can assist you with your legal information obligations and help you to respond effectively to incidents and optimise your security.

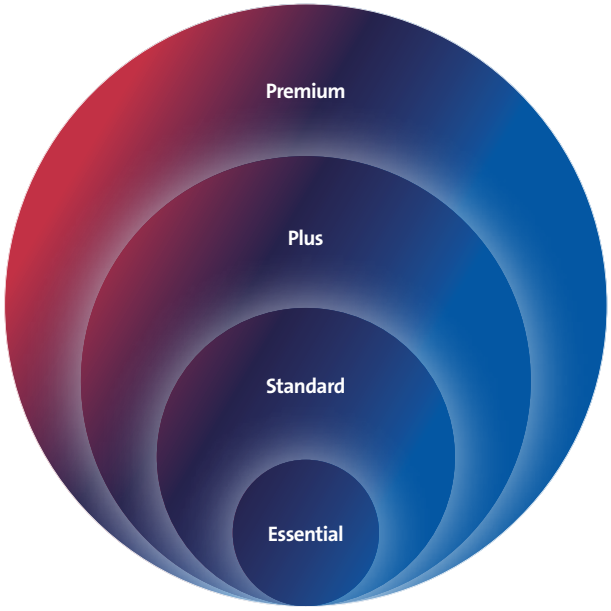
Quick, easy and independent management

Adapt your security independently, easily and centrally for all devices, company sites and users, and protect access to your company data as required. All changes instantly apply to your entire company.

Configure beem modularly and flexibly

beem is made up of three Standard components:
- **Security Editions** for comprehensive cybersecurity
- **User licences** with or without a mobile subscription
- **Company sites** with Internet, telephony and other services

By choosing the appropriate Security Edition, you can select the security functions you need based on your company's protection requirements. The functions and services provided in the Security Editions are available to all integrated users and company sites. They can be centrally managed and configured in a standardised manner for your entire company.



Security Editions & beemNet

The simple and comprehensive cybersecurity offered by beem is made possible by beemNet. This is a private, secure corporate network and your trusted gateway to the Internet. **beemNet** protects all connected devices and networks against cyber risks in real time while also reinforcing privacy protection through selective anonymisation and encryption. beemNet is also the basis for secure access to business applications and company data, both locally and in the cloud.

beemNet is operated, maintained and continually developed by Swisscom. This puts the very latest security knowledge from over 300 Swisscom security experts at your fingertips to optimally protect your company.

beemNet combines a comprehensive range of measures for protecting your business applications and sensitive data against threats from the Internet. With four redundant Swisscom data centres in Switzerland, beemNet offers high-availability, comprehensive all-round protection for employees and business partners.
Detailed information and the benefits of beemNet

The **beem Security Editions** enable you to choose scope of protection that you need for your company. The Essential Security Edition offers you secure surfing in beemNet, making it your secure gateway to the Internet. The higher-level Security Editions provide additional security functions, such as secure access to company data, device management, defence against complex cyberattacks and the prevention of data loss.
The Security Edition functions in detail (page 5)

User licences

beem user licences enable you to protect your users and their devices against cyberthreats. They also allow Zero Trust access to business applications for employees and business partners. A beem user licence gives your users access to beemNet on all devices and from all locations, integrating them into your company-wide, beem-based cybersecurity solution. Choose from a range of user licences to enable both employees and business partners to connect to beemNet. The Swisscom mobile subscriptions for business customers are seamlessly integrated into the user licences.

As soon as beemNet has been activated for your users, mobile telephones, PCs, Macs, tablets and IoT devices with a Swisscom SIM card are automatically protected in beemNet (both nationally and when roaming). Supported devices on third-party networks or public WLANs can also enjoy protection by connecting to beemNet using the beem app.

beem user licences in detail

Overview of the beem user licences

Protect & Connect
For employees

- Mobile subscription included [1]
- Security and privacy in beemNet
- Zero Trust access to business applications [2]
- Management and protection of up to 6 devices

Protect
For employees or business partners

- Security and privacy in beemNet
- Zero Trust access to business applications [2]
- Management and protection of up to 3 devices

Collaborate
For business partners

- Zero Trust access to business applications [2]

1 Available with different mobile subscriptions, for example for Europe or Switzerland. Can also be combined with NATEL® go.
2 Can be used with the beem Security Editions Standard, Plus and Premium.

Company sites

By integrating your company sites into beemNet, all connected users, devices and networks at your sites are also automatically connected to the beemNet, for example computers, mobile telephones, production machines, printers or other connected devices. Connecting company sites also enables secure access to company data or business applications on local servers from anywhere (Standard Security Edition required as a minimum), thereby eliminating the need for remote access services (RAS) or VPN solutions. Company sites are connected to beemNet using a Swisscom broadband connection for business customers, i.e. using our company site offers beem Office, Smart Business Connect or Enterprise Connect. These can be flexibly combined with add-ons such as Internet, telephony, TV, business services and other options.

beem company site offerings in detail

Security Editions in detail

Secure surfing in the beemNet	Essential	Standard	Plus	Premium
Always protected in the Swisscom network Automatic, network-based protection against cyberattacks and increased privacy for all connected devices in the mobile phone network and at company sites with a Swisscom broadband connection.	✓	✓	✓	✓
beem app for protection in third-party networks and advanced security features The beem app for client devices with Windows, MacOS, iOS, iPadOS or Android offers protection in third-party and unsecured networks (e.g. public WLANs), as well as encryption of all connections, advanced security features, device-specific push notifications in the event of cyber incidents and a personal Security Dashboard.	✓	✓	✓	✓
Increased privacy thanks to targeted anonymisation The IP addresses of connected devices are hidden from Internet services (IP cloaking). Encryption and other measures to protect employee privacy hinder social engineering and prevent targeted attacks on connected devices and networks in beemNet.	✓	✓	✓	✓
Up-to-date protection against harmful websites and malware Protection against harmful websites, phishing links, malicious file attachments, viruses, ransomware and other malware (unified threat management – UTM, secure web gateway – SWG) using deep packet inspection (DPI), even with encrypted connections (e.g. HTTPS). Swisscom security experts make adjustments to the security settings multiple times a day based on the current threat situation.	✓	✓	✓	✓
Protection against online cyberattacks Blocking of malicious online attempts to access connected networks and devices (next-generation firewall, intrusion detection & prevention system, IP cloaking, application obfuscation, zero-day prevention, etc.).	✓	✓	✓	✓

Secure access to business applications and protection of company data	Essential	Standard	Plus	Premium
Zero Trust access minimises susceptibility to attack using granular controls Access to business applications, for example, can be restricted to verified users and client devices. Finely tuned settings make it possible to stringently control access, e.g. on the basis of location, time, device properties (device posture management), network, data confidentiality level, etc. The underlying Zero Trust network access (ZTNA) enables secure access to business applications regardless of users' locations. In some cases, Zero Trust access can also be used in the local network on site. Zero Trust access makes remote access services (RAS) and VPN solutions obsolete.	⊗	✓	✓	✓
Zero Trust access for private business applications Private business applications and company data can be protected by means of a Zero Trust access approach. Business applications can be installed on local servers in the corporate network or in the cloud. For client devices within beemNet, Zero Trust access is supported on private applications even without the beem app. For companies without an inventory or suitable system documentation for their software solutions, the optional service beem Application Discovery can help to identify all relevant business applications and equip them with Zero Trust access.	⊗	✓	✓	✓
Zero Trust access for Software as a Service (SaaS) The applications to be protected can be simply selected based on an extensive catalogue of Software as a Service (SaaS) applications. There are two options available for each SaaS application: with and without user federation for single sign-on (SSO) authentication. With the first option, a reverse proxy enables protected access for client devices on the Internet, even if the devices are unknown. With the second option, a forward proxy enables access for client devices hosted in beemNet or with the beem app installed. With both options, Zero Trust access is implemented through the use of an inline cloud access security broker (CASB).	⊗	✓	✓	✓
Zero Trust access via Internet browser For unknown client devices inside and outside beemNet, the browser-based beem Business Application Portal offers Zero Trust access to private business applications (web or remote desktop). Three remote desktop protocols are supported: virtual network computing (VNC) for Linux, Mac, Windows, Raspberry Pi, etc., remote desktop protocol (RDP) for Windows and secure shell (SSH) in order to securely send commands to a computer via an unsecured network.	⊗	⊗	✓	✓

More than an SASE solution: Swisscom Enterprise Connect combined with beem Swisscom Enterprise Connect, with its extensive software-defined networking (SDN) features, IP-Plus®, SD-LAN and SD-WAN, can be combined seamlessly with beem. The combination with the beem functions for security service edge (SSE), identity & access management (IAM) and unified endpoint management (UEM) creates a custom networking and security solution with a functional range that goes beyond that of a secure access service edge (SASE) solution.	⊗	⊗	✓	✓
Information security for confidential and entrusted data Data Loss Prevention (DLP) protects confidential and sensitive data against unauthorised disclosure, data exfiltration and exposure. Automated safeguards — including encryption, quarantine, redaction and tokenisation — enable security policies to be enforced based on data classification and risk level. For data in transit, DLP policies are applied via the Secure Web Gateway (SWG). API-based data protection (API DP) extends this control to data at rest within SaaS and IaaS applications. Through direct API integrations, content and user activity are analysed, sensitive data is identified, and policies governing sharing, access and data actions are enforced. Sensitive information is detected using methods including pattern matching, exact data match and AI-based analysis.	⊗	⊗	⊗	✓

Enable and protect inbound Internet traffic	**Essential**	**Standard**	**Plus**	**Premium**
Connect and protect local (web) servers Anonymous users can access local (web) servers from the Internet by means of fixed IP addresses or through the use of dynamic DNS (DynDNS) subject to the prerequisite that the (web) server's site is connected to beemNet via a Swisscom broadband connection. Security guidelines can be established for each fixed IP address or public domain name (FQDN). The inbound Internet traffic (ingress or OUT-2-IN) is forwarded to the final host in the LAN by the Swisscom Centro Business router's built-in tools. This eliminates the need for a local firewall.	⊗	✓	✓	✓

Connect and protect (web) servers in the corporate network beem expands a corporate network based on Swisscom Enterprise Connect to include Swisscom Central Internet with or without IP Plus® and assigned fixed IP addresses. By substituting the Internet, beemNet makes it possible to control access by anonymous users to (web) servers that are accessible in the SD-WAN. Security guidelines can be established for each fixed IP address or public domain name (FQDN). The inbound Internet traffic (ingress or OUT-2-IN) is forwarded to the final host (data centre, cloud, company site) using SD-WAN or site-to-site tunnels. This means that the (web) servers requiring protection no longer need firewalls.	⊗	⊗	✓	✓
Security and optimum latency for inbound and outbound Internet traffic Swisscom Internet IP-Plus® offers technically optimal latency for access to and from the Internet (ingress and egress). beem expands IP-Plus® and replaces the Internet with beemNet. The centrally defined beem security pollicies are implemented using hardware (uCPE) on site. This combines the benefits of IP-Plus® with the comprehensive security of beem and eliminates the need for a local firewall.	⊗	⊗	✓	✓
Connect and protect e-mail traffic The secure e-mail gateway protects inbound and outbound e-mail traffic seamlessly within your existing e-mail services. Acting as an SMTP-based proxy, it routes traffic through the central beem protection instance, where e-mail content, attachments and URLs are analysed proactively, and security policies are enforced via Adaptive Threat Defence (ATD) and Data Loss Prevention (DLP).	⊗	⊗	⊗	✓

Client devices and users	**Essential**	**Standard**	**Plus**	**Premium**
Device management and security requirements for client devices Comprehensive management functions for client devices with Windows, macOS, iPadOS, iOS and Android operating systems. It is possible to block devices remotely or to delete company data stored on them. Choose from predefined Device Policies that are continuously updated by Swisscom security experts (unified endpoint management). Also suitable for combination with Swisscom Enterprise Mobility Management (EMM) or Microsoft Intune.	⊗	✓	✓	✓
Passwordless authentication and comprehensive user management Company-wide identity and access management and quick, passwordless and phishing-resistant authentication based on simple, secure passkeys. The combination with beem device management enables even the strictest of security standards (e.g. NIST AAL3) to be supported (supervised passkeys, hardware passkeys). Alternatively, customers' own, existing identity services (e.g. Microsoft Entra ID) can be used for single sign-on (SSO) authentication through federation.	⊗	✓	✓	✓

Protection against complex attacks	Essential	Standard	Plus	Premium
Secure access for all devices with remote browser isolation Remote Browser Isolation (RBI) provides comprehensive protection against web-based threats by routing all browser activity through an isolated virtual environment within beemNet. This makes devices already protected by beem even more secure, prevents unwanted data loss, and enables unmanaged devices to access business applications and corporate data securely.	⊗	⊗	optional	optional
Comprehensive protection (Security Service Edge) for IoT All SIM-based Internet of Things (IoT) devices with a Swisscom IoT contract are automatically integrated into beemNet without the need for software installation. This applies whether the devices are being used in the Swisscom mobile network in Switzerland or internationally (roaming). beem identifies the IoT devices using the international mobile subscriber identity (IMSI) and automatically creates a continually updated inventory. IMSIs can be grouped and assigned to individual security policies with the full range of functions from beem Security Service Edge. These same functions are also available for all SIM-enabled devices connected to beemNet. For example, mobile telephones, tablets, watches etc. including machine-to-machine communication (M2M).	⊗	⊗	✓	✓
AI-based detection of and defence against complex cyberattacks Adaptive Threat Defence (ATD) offers comprehensive protection against the latest cyberthreats such as zero-day attacks and ransomware. It combines AI-driven threat analysis, multi-sandbox technologies and a multi-layer security strategy to detect and neutralise threats in real time.	⊗	⊗	⊗	optional

Security guidelines and analytics	Essential	Standard	Plus	Premium
Push notifications and Security Dashboards create transparency for everyone Users receive device-specific push notifications in real time as well as a personal Security Dashboard in the beem app informing them of previously blocked content and averted cyber incidents. A Security Dashboard for administrators provides aggregated and anonymised data at company level. This creates transparency for both users and administrators.	✓	✓	✓	✓
Comprehensive analysis options to enable sound decision-making beem Analytics provides an insight into comprehensive network and security data. This enables real-time detection of threats, optimisation of network performance, prevention of shadow IT and sound decision-making. AI-based analytics (UEBA) and a connection to Swisscom Threat Detection & Response (TDR) are offered as options.	⊗	✓	✓	✓
Company-wide security policies and self-service All company-wide security policies can be managed once, centrally, for all of beemNet and all connected devices, users, access rights, networks and sites. In addition, users can be prompted to complete activities (e.g. client device onboarding), which they can subsequently do by themselves.	⊗	✓	✓	✓
Customised, individual security policies Administrators can configure customised, company-wide security policies from a central point; for instance for Zero Trust access, Unified Threat Management (UTM), Domain Name System (DNS), Data Loss Prevention (DLP) or Adaptive Threat Defence (ATD).	⊗	⊗	✓	✓

Service levels	Essential	Standard	Plus	Premium
Availability Availability guarantee for central beemNet protection.	**Best Effort**	99.9%	99.9%	99.9%
Service desk Monday-Sunday round the clock (24/7) Receives incident reports and support requests from the company administrator, not service end users.	✓	✓	✓	✓
Support times Monday-Friday, 7 am-6 pm	✓	✓	✓	✓
Monday-Saturday 6 am-10 pm (Surcharge depends on the Security Edition capacity profile)	⊗	optional	optional	optional
Monday-Sunday round the clock (24/7) (Surcharge depends on the Security Edition capacity profile)	⊗	optional	optional	optional

For more information and to contact our experts, please visit
www.swisscom.ch/beem